AMENDMENTS TO THE CLAIMS

The following is a complete listing of the claims indicating the current status of each claim and including amendments currently entered as highlighted.

Claims 1-27 (canceled)

Claim 28 (currently amended) A method for protection of computerized data, the method performed by a first user of a first computational device and a second user of ~~at least one~~a second computational device, the method comprising the steps of:

(a) randomly selecting ~~by the first user~~ a plurality of random points thereby generating a random map, wherein said selecting is performed on said first computational device by the first user;

(b) randomly fragmenting the computerized data into a plurality of fragments based on said map, each said fragment including a portion of the computerized data, said fragmenting performed by said first computational device;

(c) randomly shifting said fragments thereby encrypting the computerized data into encrypted computerized data, wherein said shifting, being performed by said first computational device is based on said map, wherein said shifting disorders the computerized data; and

(d) creating a first key based on said map, wherein said first key is operative for decrypting said encrypted computerized data by the second ~~user~~computational device.

Claim 29 (currently amended) The method according to claim 28, wherein the first computational device computational device has at least one network connection,

further comprising the step of prior to said selecting:

(e) pausing said at least one network connection.

Claim 30 (currently amended) The method according to claim 28, wherein the ~~at least one~~first computational device has at least one application running, further comprising the step of prior to said selecting:

(e) pausing said at least one application.

Claim 31 (previously presented) The method, according to claim 28, wherein said encrypting further includes scrambling said portions of the computerized data within each said fragment, said scrambling according to said map.

Claim 32 (previously presented) The method, according to claim 28, wherein at least one portion of said encrypted computerized data is not readable prior to said decrypting.

Claim 33 (previously presented) The method, according to claim 28, further comprising the step prior to said fragmenting:

(e) scrambling the computerized data according to said map.

Claim 34 (previously presented) The method, according to claim 28, wherein said generating a random map is performed using a fractal defined by a plurality of fractal parameters, wherein said encrypting is based on said fractal parameters.

Claim 35 (previously presented) The method, according to claim 28, wherein a correct order of said fragments are determined according to said map, such that solely with

use of said map, said fragments can be reassembled in said correct order subsequent to said fragmenting.

Claim 36 (previously presented) The method, according to claim 28, wherein said generating a random map includes dividing said random map into a plurality of map portions and distributing said map portions among said fragments.

Claim 37 (previously presented) The method, according to claim 28, wherein said generating a random map includes dividing said random map into a plurality of map portions wherein said first key includes varying the order of said map portions based on time.

Claim 38 (previously presented) The method, according to claim 28, wherein at least a portion of said encrypted data is concealed in an image.

Claim 39 (previously presented) The method, according to claim 28 , wherein said first key includes information about a location for storing at least a portion of the computerized data.

Claim 40 (previously presented) The method, according to claim 28 , wherein said first key includes at least a portion of said random map.

Claim 41 (previously presented) The method, according to claim 28, further comprising the steps of:

(e) transferring a copy of said first key to said second user;

(f) randomly selecting by the first user a plurality of random points thereby generating a second random map;

(g) creating a second key based on said second random map;

(h) encrypting by the first user said second key with said first key, thereby producing an encrypted second key, wherein said first key is operative to decrypt said second key by said second user.

Claim 42 (previously presented) The method, according to claim 41, wherein a plurality of sequential keys including said first key and said second key are used in sequential order, wherein at least one said sequential key is encrypted based upon at least one previous said sequential key.

Claim 43 (previously presented) The method, according to claim 42, wherein said sequential keys are used in said sequential order alternating between said first user and said second user, wherein said at least one sequential key is encrypted based further on at least one additional random map.

Claim 44 (previously presented) The method, according to claim 42, wherein at least one of said sequential keys includes location information of a next said portion of the computerized data.

Claim 45 (previously presented) The method, according to claim 42, further comprising the step of prior to said transferring, concealing at least a portion of said at least one sequential key in an image, thereby producing a modified image.

Claim 46 (previously presented) The method, according to claim 45, wherein at least a portion of said image is based on at least one fractal parameter.

Claim 47 (currently amended) A system for protection of computerized data, the comprising:

a first user and and a second user each using at least one computational device wherein said first user selects a plurality of random points thereby generating a random map;

wherein said computational device randomly fragments the computerized data into a plurality of fragments based on said map, each said fragment including a portion of the computerized data;

wherein said computational device randomly shifts said fragments based on said map and thereby ~~encrypts~~disorders the computerized data into ~~encrypted~~disordered computerized data,

wherein said computational device creates a first key based on said map, wherein said first key is operative for decrypting said ~~encrypted~~disordered computerized data by the second user.